

## CLAIMS

We claim:

1           1.     Method for the management of certificates stored on an identity module,  
2     said method comprising:  
3           providing an identity module comprising a data processing device, a storage  
4     device connected to said data processing device, a card certificate stored on the storage device,  
5     an application which uses the certificates stored on the identity module, and a data transfer  
6     device which is connected to said data processing device and which is provided with a  
7     communication interface for the transfer of information between an external device and the  
8     identity module,  
9           receiving a certificate to the identity module;  
10          authenticating said certificate by means of said card certificate; and  
11          storing information obtained from said authenticated certificate on said storage  
12     device.

1           2. Method according to claim 1, further comprising filtering said authenticated  
2     certificate to remove a certification chain contained in said authenticated certificate.

1           3. Method according to claim 1, wherein said certificate is authenticated by  
2     means of the card certificate before its use.

1           4. Method according to claim 1, wherein said stored information comprises a  
2     public key and an associated identity.

1                   5. Method according to claim 1, further comprising verifying whether said  
2 certificate is authentic prior to storage, and when authenticity cannot be verified, rejecting said  
3 certificate.

1                   6. Method according to claim 1, further comprising verifying whether said  
2 certificate is authentic before its use, and when authenticity cannot be verified, rejecting said  
3 certificate.

1                   7. Method according to claim 2, wherein the filtering comprises verifying  
2 whether each signature in said certificate is authentic, and filtering out only signatures that the  
3 verification proves to be authentic.

1                   8. Identity module for the management of certificates, said identity module  
2 comprising:

3                   a data processing device;

4                   a storage device connected to said data processing device;

5                   a card certificate stored on the storage device;

6                   an application which uses certificates;

7                   a data transfer device, which is connected to said data processing device and

8 which is provided with a communication interface for the transfer of information between an  
9 external device and the identity module;

10                  means for receiving a certificate to the identity module;

11 means for authenticating said certificate by means of said card certificate; and  
12 means for storing information contained in said authenticated certificate on said  
13 storage device.

1 9. Identity module according to claim 8, wherein the identity module further  
2 comprises:

3 means for filtering out from the certificate a certification chain contained in  
4 said authenticated certificate.

1 10. Identity module according to claim 8, wherein the identity module further  
2 comprises means for establishing the authenticity of said certificate by means of a card  
3 certificate before its use.

1 11. Identity module according to claim 8, wherein the identity module further  
2 comprises:

3 means for verifying whether said certificate is authentic prior to storage  
4 indicates that it is unreliable; and

5 means for rejecting said certificate when authenticity cannot be verified.

1 12. Identity module according to claim 8, wherein the identity module further  
2 comprises:

3 means for verifying whether said certificate is authentic prior to use; and

4 means for rejecting said certificate when authenticity cannot be verified.

1                    13. Identity module according to claim 9, wherein the identity module further  
2       comprises means for verifying the authenticity of each signature contained in said certificate  
3       before filtering.

4